REMARKS/ARGUMENTS

Favorable reconsideration of this application as presently amended and in light of the following remarks is respectfully requested.

Claims 1-4 and 11-14 remain active in this application, Claims 5-10 and 15-20 having been amended by the present amendment.

In the outstanding Office Action Claims 1-5, 8, 11-15 and 18 were rejected under 35 USC §103(a) as being unpatentable over Ugon et al (US 6,839,849) in view of Feyt et al (US 6,698,662), and Claims 6-7, 9-10, 16-17 and 19-20 were rejected under 35 USC §103(a) as being unpatentable over Ugon et al in view of Feyt et al as applied to Claims 1-5, 8, 11-15 and 18 above, and further in view of Schneier, B., Applied Cryptography, 1996, 2nd Edition, P197-206 and P372-375.

To reduce issues and expedite examination, the present amendment cancels Claims 5-10 and 15020 without prejudice.

Applicants respectfully traverse the outstanding grounds for rejection on the basis that the applied prior art clearly does not obviate the claimed invention. In particular, Claim 1 recites,

> 1. A data processing apparatus comprising:
> an operation processing unit having at least a read cycle period when said operation processing unit reads data from a device, and a write cycle period when said operation processing unit writes data in the device;
> a memory which performs data transmission/ reception between said operation processing unit and said memory;
> a data bus connected to said operation processing unit and said memory; and
> a pseudo-data generating circuit connected to said data bus, said pseudo-data generating circuit which generates pseudo-data and outputs the pseudo-data to said data bus in a time interval between the read cycle period and the write cycle period, between the write cycle period and the read cycle period, between two read cycle periods, or between two write cycle periods.

The invention recited in Claim 1 thus comprises a pseudo-data generating circuit connected to a data bus connecting an operation processing unit and a memory. As stated in

Claim 1, the pseudo-data generating circuit generates pseudo-data and outputs it to the data bus in a time interval between a read cycle period and a write cycle period, between the write cycle period and the read cycle period, between two read cycle periods, or between two write circle periods, thereby preventing secret data from leaking by applying the pseudo-data to the same data bus connected to the memory and the operation processing unit whereby operation of the latter noted units is mimicked by the pseudo-data.

Ugon et al. disclose,

> ... [a] smart integrated circuit ... constituted by a main processor (1) and a secondary processor (2), each of the processors being connected by its respective communication (Address, Data and control) bus (3, 4) to respective memories (12, 13, 22) containing the main program (P1) and the secondary program (P2) to be executed by each of the respective main (1) and secondary (2) processors, and working registers such as, for example, volatile RAMs (11, 21). The memories connected to the secondary processor are "dummy" RAMs (DumRAM 21) and ROMs (DumROM 22), which allow the secondary processor (2) to execute tasks that are superimposed on those of the main processor (1).[1]

Ugon et al thus disclose "respective", i.e., separate, data busses for the primary and secondary processors, and does not teach the secondary processor as generating and outputting pseudo data to the data bus of the primary processor. Furthermore, Ugon et al disclose use of a random generator R1 as follows:

> In another variant of embodiment, the main processor (1) activates a timer (R3) initialized either by means of the random generator (R1) or from the content of the programmable nonvolatile memory (13, NVM). This programmable nonvolatile memory (13) can actually contain a unique number modified with each use. When the timer (R3) runs out at the end of a period that cannot be predicted from the outside, it triggers an authentication of the secondary processor (2) by the main processor (1).
>
> In another variant of embodiment, the register (R2), after having been loaded with particular information (for example coming from a memory or from the random generator (R1)), can be used to trigger an interrupt.
>
> In another variant of embodiment, a random generator (R1) is connected to the interrupt system (15) of the main microprocessor (1) in order to generate

[1] Ugon et al., column 5, lines 3-15.

> interrupts that are irregular and completely non-synchronized relative to the execution of the programs in the main processor (1). Of course, the interrupt system may or may not be maskable, depending on the process in question. In this case, if the interrupt is masked, the operation of the assembly is conventional, in the single-processor mode, but as soon as the current main program (P1) wants to protect itself against possible observation, it authorizes this interrupt, which triggers the authentication and activation of the secondary processor (2). [2]

Ugon et al. in these passages disclose that the random number produced by R1 can be used in triggering an authentication of the secondary processor by the primary processor or otherwise as a trigger to interrupt the main processor. The random number is not output to a data bus, and it is respectfully submitted that Ugon et al. does not disclose any structure or functionality corresponding to the pseudo-data generating circuit recited in Claim 1.

It is respectfully submitted that the deficiencies of Ugon et al. are not remedied by the teachings of Feyt et al. or Schneier, and accordingly, it is respectfully submitted that a prima facie case of obviousness has not been made by the applied references. Therefore it is respectfully submitted that Claim 1, and the remaining claims which also recite features directed to a pseudo-data generating circuit connected to a data bus connecting an operation processing unit and a memory, are patentably distinguishing over the cited prior art.

Consequently, in view of the above comments, no further issues are believed to be outstanding, and the pending claims are believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

[2] Id., column 11, lines 13-37.